Bug 2427147 (CVE-2026-0603) - CVE-2026-0603 org.hibernate/hibernate-core: Hibernate: Information disclosure and data deletion via second-order SQL injection

Keywords: Security

Status: NEW

Alias: CVE-2026-0603

Deadline: 2026-01-31

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ depends on / blocked

Reported: 2026-01-05 13:16 UTC by OSIDB Bzimport

Modified: 2026-04-08 11:11 UTC (History)

CC List: 70 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments	(Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2026:4915	0	None	None	None	2026-03-18 13:15:15 UTC
Red Hat Product Errata	RHSA-2026:4916	0	None	None	None	2026-03-18 13:16:54 UTC
Red Hat	RHSA-2026:4917	0	None	None	None	2026-03-18

Product Errata						13:17:07 UTC
Red Hat Product Errata	RHSA-2026:4924	0	None	None	None	2026-03-18 13:55:40 UTC
Red Hat Product Errata	RHSA-2026:6011	0	None	None	None	2026-03-30 01:21:00 UTC
Red Hat Product Errata	RHSA-2026:6012	0	None	None	None	2026-03-30 01:09:38 UTC

OSIDB Bzimport 2026-01-05 13:16:50 UTC Description

I found a second order SQL Injection that I think is interesting enough to report.
On line 27 of Hibernate's InlineIdsOrClauseBuilder, the value we put into the Id column will be reused unsanitized. We do have to activate it as described here: https://in.relation.to/2017/02/01/non-temporary-table-bulk-id-strategies/#inlineidsorclausebulkidstrategy. If the user is able to set their own ids and those ids allow non-alphanumeric characters (My POC needs these: {, }, :, \", \', =) and they are using InlineIdsOrClauseBuilder then the Application is vulnerable to attack. I have provided hibernate-poc-2.zip with a vulnerable hibernate application along with 2 python scripts as POCs. In my POCs I am able to delete all items in the table with a simple id (see hibernate-poc-attack1.py in the zip), and with a slightly more complicated Id I am able to read the first 100 characters of from the

/etc/passwd

file (see hibernate-poc-attack2.py in the zip).

Octavia 2026-02-12 07:22:56 UTC Comment 4

As documented in Hibernate’s official blog regarding the InlineIdsOrClauseBulkIdStrategy
https://in.relation.to/2017/02/01/non-temporary-table-bulk-id-strategies/#inlineidsorclausebulkidstrategy
http://subwaycity.org
 - enabling this strategy causes identifier values to be inlined directly into generated SQL. If user-controlled identifiers containing non-alphanumeric characters are persisted and later reused, this may result in a second-order SQL injection condition.

errata-xmlrpc 2026-03-18 13:15:10 UTC Comment 6

This issue has been addressed in the following products:

  Red Hat JBoss Enterprise Application Platform 7.4 ELS on RHEL 7

Via RHSA-2026:4915 https://access.redhat.com/errata/RHSA-2026:4915

errata-xmlrpc 2026-03-18 13:16:49 UTC Comment 7

This issue has been addressed in the following products:

  Red Hat JBoss Enterprise Application Platform 7.4 ELS on RHEL 8

Via RHSA-2026:4916 https://access.redhat.com/errata/RHSA-2026:4916

errata-xmlrpc 2026-03-18 13:17:02 UTC Comment 8

This issue has been addressed in the following products:

  Red Hat JBoss Enterprise Application Platform 7.4 ELS on RHEL 9

Via RHSA-2026:4917 https://access.redhat.com/errata/RHSA-2026:4917

errata-xmlrpc 2026-03-18 13:55:35 UTC Comment 9

This issue has been addressed in the following products:

  Red Hat JBoss Enterprise Application Platform 7.4

Via RHSA-2026:4924 https://access.redhat.com/errata/RHSA-2026:4924

errata-xmlrpc 2026-03-30 01:09:32 UTC Comment 10

This issue has been addressed in the following products:

  Red Hat JBoss Enterprise Application Platform 7.1 EUS for RHEL 7

Via RHSA-2026:6012 https://access.redhat.com/errata/RHSA-2026:6012

errata-xmlrpc 2026-03-30 01:20:54 UTC Comment 11

This issue has been addressed in the following products:

  Red Hat JBoss Enterprise Application Platform 7.3 EUS for RHEL 7

Via RHSA-2026:6011 https://access.redhat.com/errata/RHSA-2026:6011

Note

You need to log in before you can comment on or make changes to this bug.